Security Enhancement of Medical Imaging via Imperceptible and Robust Watermarking

Manuel CEDILLO HERNANDEZ1, Antonio CEDILLO HERNANDEZ1, Francisco GARCIA UGALDE2, Mariko NAKANO MIYATAKE3, Nonmembers, and Hector PEREZ MEANA3, Member

SUMMARY In this letter we present an imperceptible and robust watermarking algorithm that uses a cryptographic hash function in the authentication application of digital medical imaging. In the proposed scheme we combine discrete Fourier transform (DFT) and local image masking to detect the watermark after a geometrical distortion and improve its imperceptibility. The image quality is measured by metrics currently used in digital image processing, such as VSNR, SSIM and PSNR.

key words: digital watermarking, medical imaging, authentication

1. Introduction

An interesting scheme recently emerged to enhance the security, confidentiality and integrity of digital medical images consisting of the use of digital watermarking in conjunction with cryptographic algorithms [1]. This solution allows the user to verify that the medical images belong to the correct patient and comes from a dependable information source which is an important property of a picture archiving and communication system (PACS) used in healthcare. Medical imaging requires extreme care when it is processed by a watermarking algorithm [2], because the additional information of the watermark may affect the image content and as a consequence it may lead to an erroneous clinical diagnostics. Nowadays, medical imaging infrastructure produces images in digital format through DICOM format (2003 standard for digital imaging and communications in medicine), which is a standard that allows the manipulation, transmission and storage of them [1]. Given the advances in information technologies as well as in security requirements, in order to avoid the undesirable but probable detachment of the image and their electronic patient record [3], we propose the use of a cryptographic hash of the DICOM metadata as the watermark to be embed into the medical images.

This letter proposes an imperceptible and robust watermarking algorithm that improves the scheme proposed in [8] as follows: a) the watermark imperceptibility has been improved without affect the robustness, replacing the integrated optical density concept implemented in [8] by a spatial masking which is described later. b) The new method has been designed to protect medical images against the practical signal processing offered in the tools included on DICOM CD Viewer display interface. Evaluation results provided show the desirable features of the proposed scheme.

2. Proposed Method

The proposed method gives the imperceptible and robust watermarking and is explained in the following steps: Watermark generation stage: 1) Read the DICOM file, extracts the desirable key information from the metadata, e.g., patient name, age, etc., and apply the message digest algorithm RIPEMD-160 [4] to obtain a hash. 2) Split the binary representation of the cryptographic hash into two parts of the same length (80 bits) and applies an XOR operation between them; obtaining then a watermark pattern W of length L = 80 bits that is directly dependent on the DICOM metadata. Watermark embedding stage: 1) Read the original DICOM image I(x, y) in a 8-bit grayscale intensity representation and rescale it into a size of N1 × N2, these dimensions will be stored and provided as a secret key K1 in the extraction stage. 2) Apply the 2D DFT denoted as $F(u, v)$ to the resized image $I(x, y)$ and obtain its magnitude $M(u, v) = |F(u, v)|$ and phase $P(u, v)$. 3) Once that Fourier spectrum has been centered, based on the energy distribution in the DFT domain, select a pair of radius $r_1$ and $r_2$ around the zero frequency term in $M(u, v)$ and compute its corresponding annular area $A = \pi(r_2^2 - r_1^2)$ that should cover the middle frequency components. Reasons of positioning $r_1$ and $r_2$ in the middle frequencies are: a) modifications in the low frequencies of $M(u, v)$ will cause a visible distortion in the spatial domain of the host image, b) modifications in the high frequencies of $M(u, v)$ may affect considerably the robustness against JPEG compression. In order to preserve the robustness respect to JPEG and at the same time keep a high visual quality, the goal then is to find a correct pair of $r_1$ and $r_2$. Fortunately there are enough radiuses in the middle frequency of $M(u, v)$ that may satisfy the trade-off between robustness and imperceptibility. These radius values will be stored and provided as a secret key $K_2$ in the extraction stage. 4) According to DFT symmetrical properties, consider the 1st and 2nd quadrants of the upper half part

---

Manuscript received January 19, 2015.
Manuscript revised May 14, 2015.
Manuscript publicized May 28, 2015.

1The authors are with the Universidad Nacional Autónoma de México (UNAM), Circuito Exterior, Ciudad Universitaria, Coyocacán, 04510 Mexico City, México.
2The authors are with the Escuela Superior de Ingeniería Mecánica y Electrónica Unidad Culhuacán, Instituto Politécnico Nacional (IPN), Av. Santa Ana 1000, San Francisco Culhuacán, Coyocacán, 04430 Mexico City, México.
3Nonmembers.

a) E-mail: mcddillowdz@hotmail.com
DOI: 10.1587/transinf.2015EDL8016

Copyright © 2015 The Institute of Electronics, Information and Communication Engineers